Amendments to the Claims:

This following listing of claims will replace all prior versions and listings of claims in the application.

1. (currently amended) A method facilitating classification of data flows, comprising

monitoring, at a network device, a data flow associated with a host relative to at least one behavioral attribute;

comparing the at least one behavioral attribute observed in the monitoring step to a knowledge base of at least one known application behavior pattern, wherein the at least one known application behavior pattern corresponds to a network application classification and comprises one or more behavioral attribute parameter values indicating a pattern of expected packet sizes for one or more packets of a data flow corresponding to the network application classification; and

classifying the data flow into [[a]] the network application classification by matching packet sizes of packets of the data flow to the pattern of expected packet sizes ~~based on the comparing step~~.

2. (canceled)

3. (currently amended) The method of claim 1 wherein the ~~at least one behavioral attribute is~~ pattern of expected packet sizes includes a packet size of the first packet in the data flow corresponding to the network application classification.

4. (currently amended) The method of claim 1 wherein the ~~at least one behavioral attribute is~~ pattern of expected packet sizes includes a packet size of the second packet in the data flow corresponding to the network application classification.

5. (currently amended) The method of claim 1 wherein the ~~at least one behavioral attribute is~~

pattern of expected packet sizes includes packet sizes for a ~~size of~~ plurality of packets in the data flow corresponding to the network application classification.

6. (currently amended) A method facilitating classification of data flows, comprising

monitoring, at a network device, a data flow associated with a host relative to at least one behavioral attribute;

comparing the at least one behavioral attribute observed in the monitoring step to a knowledge base of at least one known application behavior pattern, wherein the at least one known application behavior pattern corresponds to a network application classification and comprises one or more behavioral attribute parameter values indicating a pattern of expected ~~The method of claim 1 wherein the at least one behavioral attribute is the~~ information density associated with at least one packet in the data flow corresponding to the network application classification, wherein the information density corresponds to a level of randomness of data of the at least one packet; and

classifying the data flow into the network application classification by matching information density of packets of the data flow to the pattern of expected information density.

7. (currently amended) The method of claim [[1]] 6 wherein the ~~at least one behavioral attribute is~~ pattern of expected information density comprises the information density associated with the first packet in the data flow~~, wherein the information density corresponds to a level of randomness of data of the at least one packet~~.

8. (currently amended) The method of claim 1 wherein [[the]] at least one behavioral attribute parameter value of the one or more behavioral attribute parameter values indicates [[is]] the timing of the data flow relative to at least one similar data flow associated with the host.

9. (currently amended) The method of claim 1 wherein [[the]] at least one behavioral attribute parameter value of the one or more behavioral attribute parameter values indicates

[[is]] the number of related data flows associated with the host.

10. (currently amended) The method of claim 1 wherein [[the]] at least one behavioral attribute parameter value of the one or more behavioral attribute parameter values indicates [[is]] the timing between at least two packets in the data flow.

11. (currently amended) The method of claim 1 wherein [[the]] at least one behavioral attribute parameter values of the one or more behavioral attribute parameter values indicates [[is]] a sequence of protocol flags contained in packets of the data flow.

12. (currently amended) The method of claim 1 wherein [[the]] at least one behavioral attribute parameter values of the one or more behavioral attribute parameter values indicates a [[is]] timing of protocol flags contained in packets of the data flow.

13. (currently amended) The method of claim 1 wherein [[the]] at least one behavioral attribute parameter values of the one or more behavioral attribute parameter values indicates a ~~is the~~ timing and sequence protocol flags contained in packets of the data flow.

14. (original) The method of claim 1 wherein the application behavior pattern comprises at least one instance of any one of the following: a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows.

15. (original) The method of claim 1 wherein the application behavior pattern characterizes the first group of packets of a data flow associated with a traffic class.

16. (original) The method of claim 14 wherein the application behavior pattern characterizes the first group of packets of a data flow associated with a traffic class, and wherein the first group of packets are characterized in relation to at least one instance of any one of the following:

a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows.

17. (currently amended) A method facilitating classification of data flows, comprising

modeling behavior of a network application to generate an application behavior pattern corresponding to the network application; and

configuring a network traffic monitoring device to monitor data flows relative to at least one behavioral attribute and classify the data flows into a traffic class of a plurality of traffic classes by comparing one or more of the data flows against the application behavior pattern; wherein the application behavior pattern comprises at least one instance of any one of the following: a ~~packet size~~ pattern of expected packet sizes for one or more packets of a data flow corresponding to the network application, a pattern of expected threshold information density values for one or more packets of a data flow corresponding to the network application, a threshold inter-flow timing value between data flows corresponding to a host, or a threshold number of related application data flows corresponding to a host.

18. (currently amended) The method of claim 17 wherein the application behavior pattern further comprises at least one instance of any one of the following: ~~a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows,~~ an inter-packet timing value between a plurality of packets of a data flow corresponding to the network application, a sequence of protocol flags in a plurality of packets of a data flow corresponding to the network application, an inter-packet protocol flag timing value corresponding to a plurality of packets of a data flow corresponding to the network application.

19. (previously amended) The method of claim 18 wherein the protocol flags are Transport Control Protocol (TCP) protocol flags.

20. (currently amended) A method facilitating classification of data flows, comprising

monitoring, at a network device, the data flows associated with a host relative to at least one application behavior model corresponding to a traffic class;

matching, at the network device, at least one of the data flows associated with the host to a traffic class, if a threshold number of the data flows match a corresponding application behavior model; wherein the application behavior model comprises at least one instance of any one of the following: a ~~packet size~~ pattern of expected packet sizes for one or more packets of a data flow corresponding to the network application, a pattern of expected threshold information density values for one or more packets of a data flow corresponding to the network application, a threshold inter-flow timing value between data flows corresponding to a host, [[or]] a threshold number of related application data flows corresponding to a host, an inter-packet timing value between a plurality of packets of a data flow corresponding to the network application, a sequence of protocol flags in a plurality of packets of a data flow corresponding to the network application, an inter-packet protocol flag timing value corresponding to a plurality of packets of a data flow corresponding to the network application.

21. (currently amended) An apparatus comprising

a packet processor operative to

detect data flows in network traffic traversing a communications path, the data flows each comprising at least one packet;

parse at least one packet associated with a data flow into a flow specification,

a traffic classification engine operative to

match the data flow to a plurality of traffic classes, wherein at least one of the plurality of traffic classes is defined by one or more matching attributes, wherein said matching attributes are explicitly presented in the packets associated with the data flows, and wherein at least one other of the traffic classes is defined by one or more application behavior patterns, wherein the application behavior patterns each comprise at least one instance of any one of the following: a ~~packet size~~ pattern of expected packet sizes for one or more packets of a data flow corresponding to a traffic class, a pattern of expected threshold information density values for one or more packets of a data flow corresponding to a traffic class, a threshold inter-flow timing

value between data flows corresponding to a host, [[or]] a threshold number of related application data flows corresponding to a host, an inter-packet timing value between a plurality of packets of a data flow, a sequence of protocol flags in a plurality of packets of a data flow, or an inter-packet protocol flag timing value between a plurality of packets of a data flow;

having found a matching traffic class in the matching step, associate the flow specification corresponding to the data flow with a traffic class from the plurality of traffic classes.

22. (canceled)

23. (previously amended) The apparatus of claim 21 wherein said flow specification contains at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a protocol type designation, a pair of hosts, a pair of ports, a pointer to a multipurpose internet mail extensions (MIME) type, and a pointer to an application-specific attribute.

24. (previously amended) The apparatus of claim 21 wherein said flow specification contains, and wherein the one or more matching attributes include, at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a protocol type designation, a pair of hosts, a pair of ports, a pointer to a multipurpose internet mail extensions (MIME) type, and a pointer to an application-specific attribute.

25. (original) The apparatus of claim 21 further comprising

a flow control module operative to apply bandwidth utilization controls to the data flows based on the traffic class associated with the data flows.

26. (currently amended) A method facilitating classification of data flows, comprising

detecting, at a network device, a data flow in network traffic traversing a communications path, the data flows each comprising at least one packet;

parsing explicit attributes at least one packet associated with the data flow into a flow specification,

matching the flow specification to a first plurality of traffic classes, wherein the first plurality of traffic classes are each defined by one or more matching attributes,

having found a matching traffic class in the matching step, associating the flow specification corresponding to the data flow with a traffic class from the first plurality of traffic classes,

not having found a matching traffic class in the first plurality of traffic classes, matching the data flow to at least one additional traffic class, the additional traffic class defined by an application behavior pattern, the application behavior pattern comprising comprises at least one instance of: a ~~packet size~~ pattern of expected packet sizes for one or more packets of a data flow, a pattern of expected threshold information density values for one or more packets of a data flow, a threshold inter-flow timing value between data flows corresponding to a host, or a threshold number of related application data flows corresponding to a host.

27. (previously amended) The method of claim 26 wherein the flow specification contains at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a protocol type designation, a pair of hosts, a pair of ports, a pointer to a multipurpose internet mail extensions (MIME) type, and a pointer to an application-specific attribute.

28. (previously amended) The method of claim 26 wherein said flow specification contains, and wherein the one or more matching attributes include, at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a protocol type designation, a pair of hosts, a pair of ports, a pointer to a multipurpose internet mail extensions (MIME) type, and a pointer to an application-specific attribute.

29. (currently amended) A method facilitating the classification of network traffic, comprising

detecting, at a network device, a data flow in network traffic traversing a

communications path, the data flow comprising at least one packet;

classifying the data flow into a network application of a plurality of network applications by

applying a mathematical function to at least one packet in the data flow to derive a computed value that characterizes entropy of information contained in the at least one packet, wherein the entropy information corresponds to a level of randomness of data of the at least one packet; and

comparing the computed value to at least one traffic class corresponding to the network application, said traffic class defined, at least in part, by a required computed entropy value.

30. (original) The method of claim 29 wherein the required computed value is determined by applying the mathematical function to data flows known to be of the traffic class.

31. (original) The method of claim 29 wherein the mathematical function computes a value indicating the information density of at least one packet.

32. (original) The method of claim 29 wherein the required computed value is a range of values.

33. (currently amended) A method facilitating the classification of network traffic, comprising

detecting, at a network device, a data flow in network traffic traversing a communications path, the data flow comprising at least one packet containing a first checksum;

applying a mathematical function to at least one packet in the data flow to derive a second checksum;

comparing the computed second checksum to the first checksum contained in the at least one packet;

matching the data flow to a traffic class, wherein the traffic class is defined at least in part by whether the computed second checksum should match the first checksum in the at least

one packet.